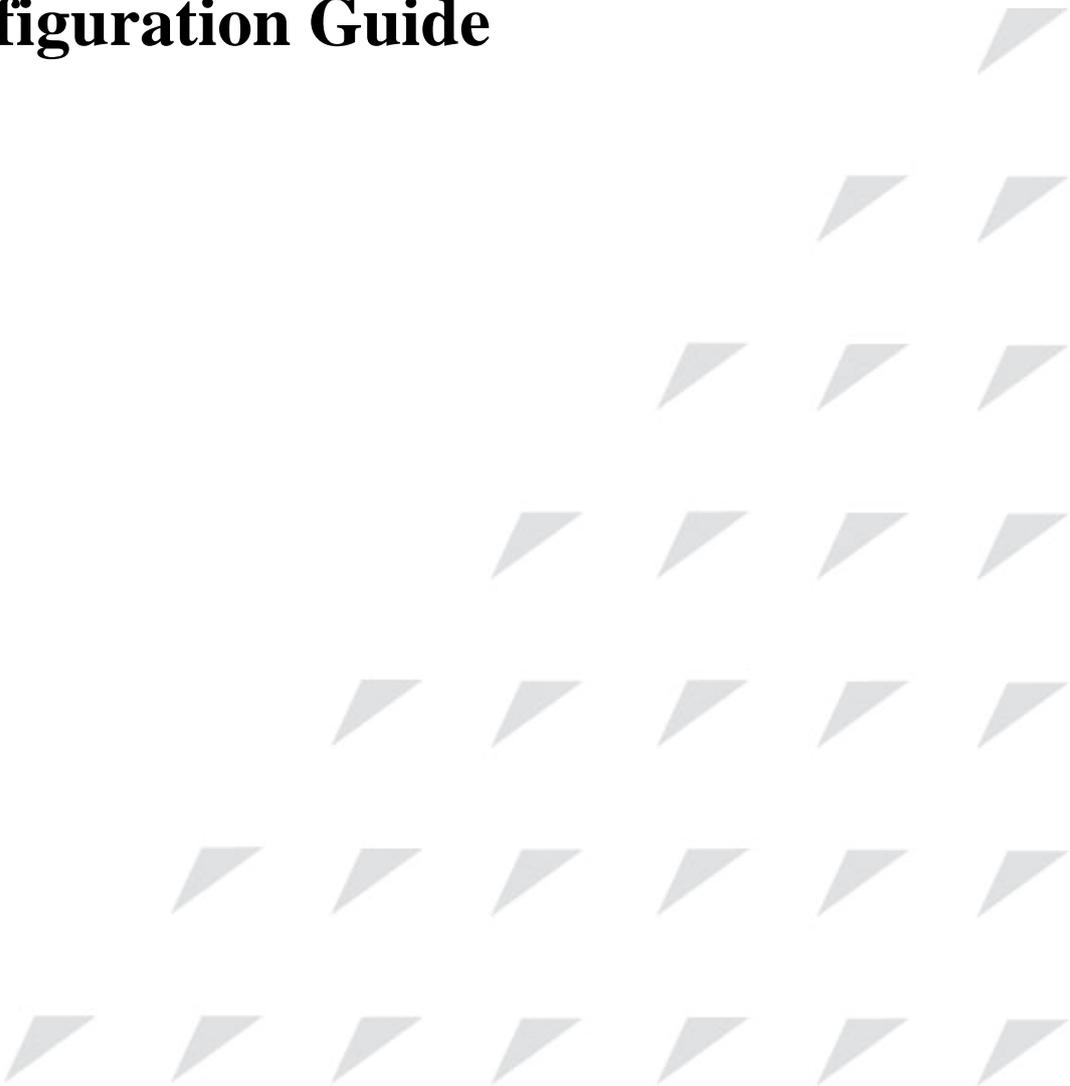


www.raisecom.com

VLAN Configuration Guide



Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

Copyright ©2007 Raisecom. All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

<http://www.raisecom.com>

Feedback

Comments and questions about how the ... system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

<http://www.raisecom.com/en/xcontactus/contactus.htm>.

If you have comments on the ... specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Release Notes	5
Chapter 1 VLAN Principle	1
1.1 IEEE802.1Q VLAN	1
1.2 VLAN Mapping interview	1
1.3 Q-IN-Q interview	2
Chapter 2 Switch VLAN Function Configuration	3
2.1 VLAN based on port	3
2.1.1 VLAN port mode interview	3
2.1.2 Default VLAN configuration	4
2.1.3 Configure VLAN Attribute	4
2.1.4 Configure VLAN priority	5
2.1.5 Configure port VLAN mode	6
2.1.6 VLAN filtration enable/disable function	10
2.1.7 Configure port protection	11
2.1.8 Configure port transmission	11
2.1.9 Monitoring and maintenance	12
2.1.10 Typical configuration example	12
2.2 VLAN mapping function	14
2.2.1 Default VLAN mapping configuration	14
2.2.2 Configure VLAN mapping	14
2.2.3 Monitoring and maintenance	15
2.2.4 Typical configuration example	16
2.3 Basic Q-IN-Q function	17
2.3.1 Default Q-IN-IN configuration	17
2.3.2 Basic Q-IN-Q configuration	17
2.3.3 Monitoring and maintenance	18
2.3.4 Typical configuration example	19
2.4 Flexible Q-IN-Q function	22
2.4.1 Default flexible Q-IN-Q configuration	22
2.4.2 Configure flexible Q-IN-Q	22
2.4.3 Monitoring and maintenance	23
2.4.4 Typical configuration example	23
Chapter 3 VLAN Function Configuration	28
3.1 Configure VLAN	28
3.1.1 Switching mode introduction	28
3.1.2 Default VLAN configuration	28
3.1.3 Configure switching mode	28
3.1.4 Configure VLAN attribute	29
3.1.5 Enable/disable VLAN filtration	30
3.1.6 Configure VLAN accept-frame tagging type	30
3.1.7 Configure outgress mode	31
3.1.8 Configure PVID	32
3.1.9 Monitoring and maintenance	32
3.1.10 Typical configuration example	33
3.2 Basic Q-in-Q function	35
3.2.1 Basic Q-in-Q default configuration	35
3.2.2 Configure basic Q-in-Q	35
3.2.3 Monitoring and maintenance	36
3.2.4 Typical configuration example	36

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of ... device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《... User Manual》

《... Commands Notebook》

Organization

This manual is an introduction of the main functions of ... EMS. To have a quick grasp of the using of the EMS of ... , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of ...

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the

Chapter 3 Performance Management

This chapter focuses on performance management function of

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of

Appendix A Alarm Type

The alarm types supported by

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules—2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules—2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

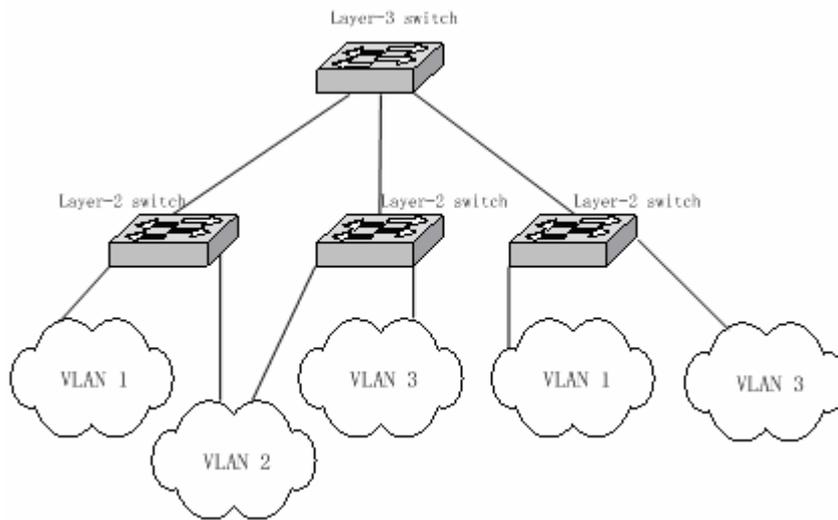
IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 VLAN Principle

1.1 IEEE802.1Q VLAN

VLAN stands for virtual LAN (virtual Local Area Networks). In terms of functions, VLAN has the same characteristics with LAN. However, VLAN members are not restricted by physical locations. For instance, the users connected to the same switch can belong to different VLANs. The broadcast domain and multicast domain are both in reference to VLAN member, multicast, broadcast and unicast will not flood to other VLANs. Different VLANs can communicate with each other only via Layer-3 switch or router. The features above offer much convenience for network management, user can allocate VLANs based on functions in the network so as to promote the network bandwidth utility and security. A typical VLAN network topology is shown below:



VLAN, a protocol to handle the Ethernet problems from broadcasting and safety, is added VLAN port based on Ethernet frame, divides users into smaller working group using VLAN ID and limits the two-layer visit between users within different working groups. Each working group is a virtual LAN.

In 1999 IEEE issues the 802.1Q protocol standard draft for VLAN realization project. As the criterion of VLAN, it encapsulates VLAN ID in the frame header, so that the VLAN information can be kept when a frame is crossing different equipments. The switches of different producers can be under unified management and cross switches if only they support 802.1Q VLAN.

1.2 VLAN Mapping interview

VLAN Mapping can modify VLAN Tag in the message, and supports the following two mapping relationships:

- 1: 1VLAN Mapping: change the VLAN ID in VLAN Tag taken by a message into another VLAN ID.
- 2: 2VLAN Mapping: add out-layer VLAN Tag to the message with one layer VLAN Tag, so that the message can take two layer VLAN Tag.

1.3 Q-IN-Q interview

In the framework of IP data network, the switch is used as access equipment, when LAN is used as the access process, to divide users for user's data safety becomes a serious problem.

Now many producers demands end to end safety recognition, hoping each user can allocated a VLAN, but the problem is that there are only 4096 standard VLAN resources. However, using the innovative Q-in-Q technology, the limit of 4096 VLAN can be broken through in metro Ethernet assembly, which not only extends the ability of creating two-layer network using VLAN, but also realizing metro network two-layer VPN, that is suitable for metro network and WAN services.

Q-in-Q technology is a simple and flexible two-layer VPN technology. Using outer-layer VLAN Tag to encapsulate outer-layer VLAN Tag for user's private network message in carrier's access end, it can let the message carry two-layer VLAN Tag to cross carrier's backbone network (public network). Inner layer VLAN Tag is user private network VLAN Tag, outer layer VLAN Tag is the one that carrier allocates to user. In public network, messages transmit only according to the outer layer VLAN Tag, and the source MAC address table item of the messages is learned and copied to the MAC address table of the VLAN that outer layer Tag is in, while user's private network VLAN Tag will be taken as the messages' data part for transmission.

The basic working principle and method of Q-in-Q: when the data is transmitting in private network it has a private network mark, defined as CVLAN Tag; when entering the backbone network of facilitator, public network VLAN Tag will be added to it, defined as SPVLAN Tag (or Outer tag); when reaching destination private network the SPVLAN Tag of the public network will be deleted to offer user a relatively simple two-layer VPN tunnel. SPVLAN Tag is embedded after Ethernet source MAC address and destination MAC address, which also contains a 12 bits SPVLAN ID that supports 4096 VLAN. SPVLAN CoS domain contains 3 bits, supports 8 priority. In the network based on Q-in-Q, the operator allocates a SPVLAN ID for each VLAN, then maps user's CVLAN ID to these SPVLAN ID. Thus, user's C-VLAN ID can be protected.

Chapter 2 Switch VLAN Function Configuration

2.1 VLAN based on port

VLAN division based on port is the most simple and effective way for VLAN division. It defines VLAN member according to the equipment port, and when the given port enters the given VLAN, it can transmit messages from the given VLAN

2.1.1 VLAN port mode interview

Port member mode	VLAN member attributes
Access	Under this mode, the port can be allocated to a single VLAN, packet sent from Access port does not have no 802.1Q tag, Access ports within different VLANs cannot communicate with each other.
Hybrid	Under this mode, the port can be allocated to multiple VLANs, you can also determine if packet sent out from Hybrid port carries related 802.1Q tag or not. Meanwhile, you can also classify the non-802.1Q packets that enter the port into different VLANs by setting the Native attribute of the port.
Trunk	Trunk port can be allocated with different VLANs by default, packet forwarded from it carries 802.1Q tag expect for Native VLAN. However, you can limit the packets through which VLAN they are forwarded by using <i>allowed vlans</i>
Dot1q-tunnel	TUNNEL port mode can only be designated to one VLAN by user, the data packet transmitted from TUNNEL port do not contain out layer TAG, TUNNEL port of different VLAN can not interflow. The data packet entered from TUNNEL port can be added two layer TAG.
Trunk double-tagging	Configure port to TRUNK mode, and enable the port the ability of recognizing and handling out layer TAG (that is SP VLAN TAG).
Hybrid dot1q-tunnel	Configure the port to HYBRID mode, enable the port the ability of adding outer layer TAG (that is SP VLAN TAG) for the packet entering the port (ignoring the out-layer/inner-layer TAG in the data packet)

2.1.2 Default VLAN configuration

Function	Default value
Create stable VLAN	There are default VLAN and cluster VLAN in the system, that is VLAN 1 and VLAN 2, all the ports exists in VLAN 1 in access mode
VLAN name	The default system VLAN (VLAN 1) is 'Default' , cluster VLAN name is 'Cluster-Vlan' , other stable VLAN name is 'VLAN' adding VLAN ID(four figures number)
Configure the activity state of stable VLAN	The new created stable VLAN activity state is suspend.
Configure the port mode	Access
Configure the VLAN number that is allowed to pass in HYBRID mode	All VLAN
Configure the VLAN number that is allowed to pass in TRUNK mode	VLAN1.
Configure Native VLAN for Trunk, Hybrid port	VLAN1
VLAN filtration attribute	Enable
Port protection	The port is not protected port
Transmission port list	All the other ports except its own port
VLAN priority	No priority

2.1.3 Configure VLAN Attribute

VLAN attribute configuration includes the VLAN configuration of creation, deletion, name and activity state. The configuration steps are as follows:

Step	Command	Command parameter explain
1	config	Enter global configuration mode

2	create vlan {2-4094} (active suspend) priority {0-7}	Create VLAN and make sure the state: active/suspend 0-7: VLAN priority {2-4094}: VLAN ID
3	vlan <1-4094>	Create VLAN and enter the configuration mode <1-4094> VLAN ID
4	name <i>WORD</i>	Dominate VLAN <i>WORD</i> VLAN name, no longer than 15 characters
5	state { active suspend }	Configure VLAN state: active/suspend
6	exit	Return to global configuration mode
7	exit	Return to privileged EXEC mode
8	show vlan	Show VLAN configuration

Use **no vlan** <2-4094> to delete VLAN.

△ Notice:

- The new created VLAN using VLAN <1-4094> is in suspend state, if user wishes to activate it in the system, the command **state** that would be introduced later is needed to activate VLAN.
- By default there are VLAN existed in the system, that is default VLAN (VLAN 1) and cluster VLAN (VLAN 2), all the ports are Access mode belongs to the default VLAN. VLAN priority range is 0-7.
- The new created VLAN, has no priority by default, is shown as N/A. VLAN priority range is 0-7.
- By default, default VLAN (VLAN 1) name is 'Default', cluster VLAN (VLAN 2) name is 'Cluster-VLAN', other VLAN name is character stream 'VLAN' added four figures VLAN ID. For example, the default VLAN 1 name is 'VLAN0001', the default VLAN 4094 name is 'VLAN4094'.
- All the VLAN configuration can no take effect until the VLAN is activated. When VLAN activity state is suspend, user can still configure the VLAN, like delete/add port, configure VLAN name and so on, the system will keep the configuration, once the VLAN is activated, the configuration will take effect in the system.

2.1.4 Configure VLAN priority

By default, when VLAN is created, there is no priority, shown as N/A, the VLAN priority range is 0-7. The configuration steps are as follows:

Step	Command	Command parameter example
1	config	Enter global configuration mode
2	vlan {2-4094} priority <0-7>	Configure VLAN priority {2-4094} VLAN ID <0-7> VLAN priority
3	exit	Return to privileged EXEC mode
4	show vlan	Shown VLAN configuraion

Use **no vlan {2-4094} priority** to restore VLAN priority to default state, or VLAN without priority.

2.1.5 Configure port VLAN mode

Each mode and the configuration is shown below:

1. Configure port VLAN mode

Port VLAN mode configuration must be done in physical interface configuration mode, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter the corresponding physical port configuration mode <i>portid</i> : port number
3	switchport mode {access hybrid [double-tagging] trunk [double-tagging] [hybrid] dot1q-tunnel }	Configure port VLAN mode access ACCESS mode, that is port exists in the unique VLAN in the form of UNTAG; hybrid HYBRID mode, port can exist in several VLAN in both UNTAG or TAG mode hybrid double-tagging Configure the port to HYBRID mode, and enable the port the ability of recognizing and handing outer layer Tag (or SP VLAN Tag)

		<p>hybrid dot1q-tunnel configure the port to HYBRID mode, and enable the port the ability of compulsively adding outer layer Tag (or SP VLAN Tag) for the packets.</p> <p>trunk TRUNK mode, port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode.</p> <p>trunk double-tagging configure the port to TRUNK mode so that it is able to recognize and handle outer layer Tag (or SP VLAN Tag)</p> <p>dot1q-tunnel TUNNEL mode, the data packet enters from this port can be added double Tag</p>
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [port-list] switchport	Show port VLAN attribute configuration

Use **no switchport mode** to restore port VLAN mode to default value, that is port VLAN mode is Access mode.

2. Configure Access, dot1q-tunnel port Access VLAN, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port portid	Enter physical port configuration mode
3	switchport access vlan <1-4094>	Configure VLAN that is allowed to pass Hybrid port

4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [<i>port-list</i>] switchport	Show port VLAN attribute configuration

Use **no switchport access vlan** command to restore Access VLAN to default value, or port Access VLAN is VLAN 1.

3. Configure VLAN that is allowed to pass through Hybrid port ,the steps are as follows:

Step	Comamnd	Description
1	config	Enter global configuration mode
2	interface port <1-26>	Enter the corresponding physical port configuration mode
3	switchport hybrid allowed vlan { all <i>vlan-list</i> add <i>add-vlan-list</i> remove <i>remove-vlan-list</i> }	Configure the allowed VLANs for the Hybrid port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan Remove: remove-vlan-list, remote vlan base on the existent vlan
4	switchport hybrid untagged vlan { all <i>vlan-list</i> add <i>add-vlan-list</i> remove <i>remove-vlan-list</i> }	Configure the allowed VLANs for the Untagged port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan

		Remove: remove-vlan-list, remote vlan base on the existent vlan
5	exit	Back to global configuration mode
6	exit	Back to privileged EXEC mode
7	show interface port [{1-26}] switchport	Show the port VLAN attributes configuration

Use **no switchport hybrid allowed vlan** to restore Hybrid port allowed VLAN to default value, that is, all the VLAN is allowed to pass.

Use **no switchport hybrid untagged vlan** to restore Hybrid port allowed Untagged VLAN to default value, that is, only VLAN is allowed to pass.

4. Configure VLAN that is allowed to pass Trunk port, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter corresponding physical port configuration mode
3	switchport trunk allowed vlan { all <i>vlan-list</i> add <i>add-vlan-list</i> remove <i>remove-vlan-list</i> }	Configure the allowed VLAN for the Trunk port All: allow all vlan vlan-list: allow all VLAN, rewrite the primary configuration Add: add-vlan-list: add vlan base on the existent vlan Remove: remove-vlan-list, remote vlan base on the existent vlan
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode

6	show interface port [port-list] switchport	Show port VLAN attribute configuration
----------	---	---

Use **no switchport trunk allowed vlan** to restore Trunk port allowed VLAN list to default value, that is, all the VLAN.

5. Configure Native VLAN of Trunk and Hybrid port, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port portid	Enter corresponding physical port configuration mode
3	switchport native vlan <1-4094>	Configure Native VLAN of Trunk and Hybrid port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [port-list] switchport	Show port VLAN attribute configuration

Use **no switchport native vlan** to restore Native VLAN of Trunk and Hybrid port to default value, or VLAN1.

2.1.6 VLAN filtration enable/disable function

The configuration of VLAN filtration enable/disable function is shown below:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port portid	Enter corresponding physical port configuration mode
3	switchport ingress-filtering (enable disable)	Configure port VLAN filtration attribute : enable/disable

4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port [port-list] switchport	Show port VLAN attribute configuration

2.1.7 Configure port protection

The configuration steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port portid	Enter corresponding physical port configuration mode
3	switchport protect	Configure the physical port to protected port Protect the protected port
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface port protected	Show physical port protection attribute

Use **no switchport protect** to cancel port protection configuration.

2.1.8 Configure port transmission

By default, the port can transmit messages to other ports except its own one, port transmission function supports port list configuration under port, so that the range of the ports that are able to transmit messages can be confined.

To configure transmission port, you need to enter the given port or port range mode, the corresponding commands are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port portid	Enter port mode

3	switchport forwarding allowed portlist <i>port-list</i>	Configure transmission list under port <i>Port-list:</i> port list
4	exit	Quit from interface mode
5	exit	Quit from global configuration mode
6	show interface port <i>[port-list]</i> switchport	Show port transmission list

Use **no switchport forwarding allowed portlist** to restore port transmission list to default value, that is, all the ports except its own one.

2.1.9 Monitoring and maintenance

Command	Command parameter introduction
show interface port <i>[port-list]</i> switchport	Show port VLAN attribute configuration
show interface port protected	Show physical port protection attribute
show vlan	Show port VLAN attribute configuration

2.1.10 Typical configuration example

The topology structure is shown below:



Fig 1 topology structure

As is shown in figure 1, the SwitchA and SwitchB use Port1(SwtichA) and Port1(SwitchB) to connect each other, configure Port1 of the two equipments to Trunk port, allowVLAN1-VLAN100 to pass, Port3(SwtichA) and Port3(SwtichB) are Access port, Access VLAN is VLAN6. The configuration of SwitchA and SwitchB are totally the same, now SwitchA configuration will be shown.

SwitchA configuration is as follows:

```
Raisecom#config
Raisecom(config)#vlan 6
Raisecom(config-vlan)#state active
Raisecom(config-vlan)#exit
```

```

Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 1-100
Raisecom(config-port)# exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode access
Raisecom(config-port)# switchport access vlan 6
Raisecom(config-port)#exit
Raisecom(config)#exit

```

```
Raisecom#show vlan
```

```
Outer TPID: 0x9100
```

VLAN	Name	Status	VLAN-Priority	Ports
1	Default	active	N/A	1,2,4-26
6	VLAN0006	active	0	3

```
Raisecom#show interface port 1 switchport
```

```
Port 1:
```

```
Administrative Mode: trunk
```

```
Operational Mode: trunk
```

```
Access Mode VLAN: 1(default)
```

```
Tunnel Mode VLAN: 1(default)
```

```
Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a
```

```
Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a
```

```
Administrative Trunk Allowed VLANs: 1-100
```

```
Operational Trunk Allowed VLANs: 1,3-100
```

```
Administrative Hybrid Allowed VLANs: 1-4094
```

```
Operational Hybrid Allowed VLANs: n/a
```

```
Administrative Hybrid Untagged VLANs: 1
```

```
Operational Hybrid Untagged VLANs: n/a
```

```
Native Mode VLAN: 1(default)
```

```
VLAN Ingress Filtering: Enabled
```

```
switchport forwarding allowed portlist: n/a
```

Raisecom#show interface port 3 switchport

Port 3:

Administrative Mode: access

Operational Mode: access

Access Mode VLAN: 6

Tunnel Mode VLAN: 6

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

2.2 VLAN mapping function

VLAN mapping offers CVID for message modification, if the equipment has configured the corresponding mapping rules, the new CVID or SVID that has been mapped will do learning and transmission as transmission VLAN.

2.2.1 Default VLAN mapping configuration

Function	Default value
Enable/disable port VLAN mapping function	Disable to all

2.2.2 Configure VLAN mapping

The steps to enable/disable VLAN mapping function and configure VLAN Mapping rules are shown below:

Step	Command	Command parameter explain
1		
2		
3		

1	<code>config</code>	Enter global configuration mode
2	<code>vlan-mapping <i>vlan-list1</i> to <i>vlan-list2</i></code>	Configure VLAN mapping rule <i>Vlan-list1</i> the VLAN ID before mapping <i>Vlan-list2</i> the VLAN ID afeter mapping
3	<code>interface port <i>portid</i></code>	Enter interface configuration mode
4	<code>vlan-mapping {<i>enable</i> <i>disable</i>}</code>	Enable VLAN mapping function <i>Enable</i> enable VLAN mapping <i>Disable</i> disable VLAN mapping
5	<code>exit</code>	Quit from physical port mode
6	<code>exit</code>	Quit from global configuration mode
7	<code>show vlan-mapping</code>	Show VLAN mapping rules
8	<code>show port {<i>all</i>/<i>port-list</i>} vlan-mapping</code>	Show all/specified port VLAN mapping function state <i>All</i> : all the ports <i>Port-list</i> : the specified port or port list

△ Notice:

- If the number relationship of *vlan-list1* and *vlan-list2* is $N(N>1)$ to 1, the command will map several VLAN to one VLAN; if it is N to N , then *vlan-list1* and *vlan-list2* need to be the same in amount in configuration, when doing VLAN mapping the principle of one-one correspondence.
- By default VLAN mapping function is disabled. When VLAN mapping function of the specified port is enabled, the corresponding mapping rule will take effect on the port.

2.2.3 Monitoring and maintainenance

Command	Command parameter introduction
<code>show interface port [<i>port-list</i>] switchport</code>	Show the transmission list under specified port
<code>show vlan-mapping</code>	Show VLAN mapping rules
<code>show port {<i>all</i>/<i>port-list</i>} vlan-mapping</code>	Show all/ the specified ports VLAN mapping function state <i>All</i> : all the ports

Port-list: specified port or port list

2.2.4 Typical configuration example

The topology structure is shown in figure 2:

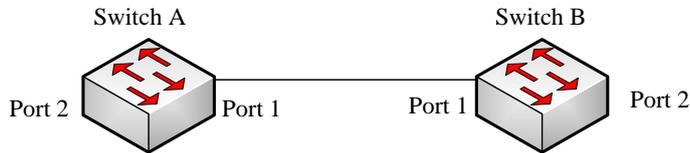


Fig 2 the topology structure

As is shown in figure 2, SwitchA and SwitchB use port 1 for connection, the Port1 and Port2 of the two equipments are both trunk port, create VLAN10-20 and 110-120, map vlan10-20 to vlan110-120, enable VLAN mapping function on Port2. The configuration of SwtichA and SwitchB is totally the same, now SwtichA configuration will be shown.

The configuration of SwitchA:

```

Raisecom#config
Raisecom(config)#create vlan 10-20, 110-120 active
Raisecom(config)# vlan-mapping 10-20 to 110-120
Raisecom(config)#interface port 1
Raisecom(config-port)# switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)# interface port 2
Raisecom(config-port)# switchport mode trunk
Raisecom(config-port)#vlan-mapping enable
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show vlan-mapping

```

Global vlan mapping rules:

Original VLAN IDs	Translated VLAN IDs

10-20	110-120

```

Raisecom#show port 1-2 vlan-mapping

```

Vlan Mapping Status:

PORT	VLAN-MAPPING STATUS

1	disable
2	enable

2.3 Basic Q-IN-Q function

2.3.1 Default Q-IN-IN configuration

Function	Default value
Configure TPID value of outer layer Tag is HHHH	Default TPID value of outer layer Tag is 0x9100
Configure the port ACCESS VLAN ID	1
Configure port VLAN mode	All the ports exists in ACCESS mode in VLAN1.

2.3.2 Basic Q-IN-Q configuration

The steps of configuring Q-IN-Q includes: Tpid, access vlan, tunnel port and double tagging configuration, as is shown below:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	mls double-tagging tpid HHHH	Configure the outer layer Tag TPID value to HHHH; <i>HHHH</i> : hex outer layer Tag TPID value, it is 1~4 figures hex number, range is 0x0-0xFFFF.
3	interface port <i>portid</i>	Enter port mode
4	switchport mode {access hybrid [double-tagging dot1q-tunnel] trunk [double-tagging] dot1q-tunnel [hybrid]}	Configure port VLAN mode access ACCESS mode, port exists in the form of UNTAG in the only VLAN; hybrid HYBRID mode, the port can exist in several VLAN in UNTAG or TAG mode; hybrid double-tagging configure

		<p>the port to HYBRID mode, so that it can recognize and handle outer layer Tag (SP VLAN Tag);</p> <p>hybrid dot1q-tunnel configure the port to HYBRID mode, can make it enable to compulsively adding outer layer Tag(SP VLAN Tag) for the packet entering the port;</p> <p>trunk TRUNK mode, the port exists in several VLAN in TAG mode, and exists in Native Vlan in UNTAG mode;</p> <p>trunk double-tagging configure the port to TRUNK mode, and enable it the ability to recognize and handle outer layer Tag;</p> <p>dot1q-tunnel TUNNEL mode, the data packet entering the port can be added double Tag.</p>
4	switchport access vlan <1-4094>	Configure the port ACCESS VLAN ID. <1-4094> specific port' s ACCESS VLAN ID in ACCESS and DOT1Q-TUNNEL mode.
5	exit	Return to global configuration mode
6	show vlan	Show VLAN configuration
7	show interface port [port-list] switchport	Show port VLAN attribute information

Use **no mls double-tagging tpid HHHH** to restore outer layer Tag TPID to default value:0x9100.

Use **no switchport mode** to restore port VLAN mode to default value, that is ACCESS mode.

Use **no switchport access vlan** mode to restore Access VLAN to default value, that is, port Access VLAN is VLAN 1.

2.3.3 Monitoring and maintenance

Command	Command parameter instruction
---------	-------------------------------

show vlan [{1-4094}]	Show stable VLAN configuration
show interface port [port-list] switchport	Show port VLAN attribute configuration

2.3.4 Typical configuration example

The topology structure is shown in figure 3:

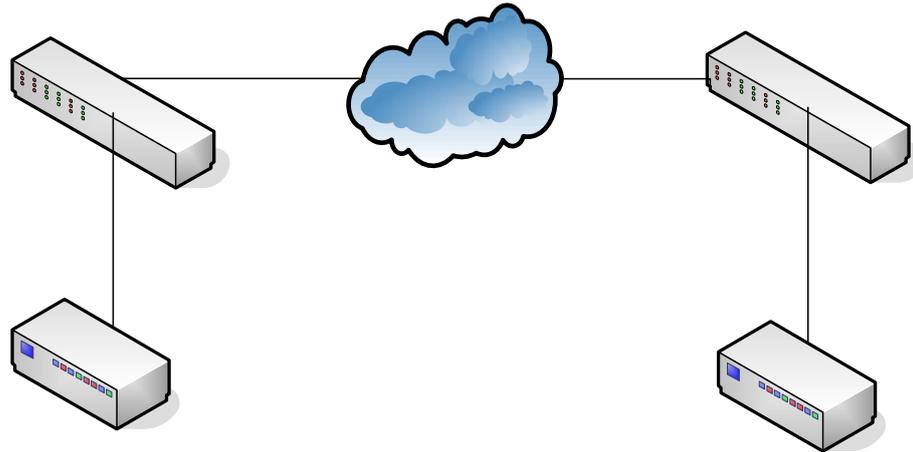


Fig 3 topology structure

As is shown in figure 3, SwitchA and SwitchB are operator access switches, belong to operator network's VLAN100 and VLAN200 respectively. User1 and User2 are user access equipment, SwitchA use P5 port to connect to MAN (metro area network), p1 port connect of User1, SwitchB use P5 to connect to MAN. P1 connect to User2. MAN TPID is 0x8600. Configure SwitchA and SwitchB to realize QinQ function.

SwitchA configuration is shown below:

```

Raisecom#config
Raisecom(config)#mls double-tagging tpid 8600
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode dot1q-tunnel
Raisecom(config-port)#switchport access vlan 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 5
Raisecom(config-port)#switchport mode trunk double-tagging
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show interface port 1 switchport

```

Port 1:

User1

Administrative Mode: dot1q-tunnel
Operational Mode: dot1q-tunnel
Access Mode VLAN: 100
Tunnel Mode VLAN: 100
Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a
Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: n/a
Administrative Hybrid Allowed VLANs: 1-4094
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 1(default)
VLAN Ingress Filtering: Enabled
switchport forwarding allowed portlist: n/a

Raisecom#show interface port 5 switchport

Port 5:
Administrative Mode: trunk double-tagging
Operational Mode: trunk double-tagging
Access Mode VLAN: 1(default)
Tunnel Mode VLAN: 1(default)
Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a
Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: 1,100
Administrative Hybrid Allowed VLANs: 1-4094
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1
Operational Hybrid Untagged VLANs: n/a
Native Mode VLAN: 1(default)
VLAN Ingress Filtering: Enabled
switchport forwarding allowed portlist: n/a

SwitchB configuration is shown below:

```
Raisecom#config
```

```
Raisecom(config)#mls double-tagging tpid 8600
```

```
Raisecom(config)#interface port 1
```

```
Raisecom(config-port)#switchport mode dot1q-tunnel
```

```
Raisecom(config-port)#switchport access vlan 200
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#interface port 5
```

```
Raisecom(config-port)#switchport mode trunk double-tagging
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#show interface port 1 switchport
```

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 200

Tunnel Mode VLAN: 200

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

```
Raisecom# show interface port 5 switchport
```

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

- Tunnel Mode VLAN: 1(default)
- Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a
- Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a
- Administrative Trunk Allowed VLANs: 1-4094
- Operational Trunk Allowed VLANs: 1,200
- Administrative Hybrid Allowed VLANs: 1-4094
- Operational Hybrid Allowed VLANs: n/a
- Administrative Hybrid Untagged VLANs: 1
- Operational Hybrid Untagged VLANs: n/a
- Native Mode VLAN: 1(default)
- VLAN Ingress Filtering: Enabled
- switchport forwarding allowed portlist: n/a

2.4 Flexible Q-IN-Q function

2.4.1 Default flexible Q-IN-Q configuration

Function	Default value
Configure port flexible Q-IN-Q VLAN mapping relationship	None

2.4.2 Configure flexible Q-IN-Q

Flexible Q-in-Q function is to add outer layer TAG according to inner TAG. Configuring port flexible Q-in-Q function must be within physical port configuration mode, the steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	interface port <i>portid</i>	Enter corresponding physical port configuration mode
3	switchport vlan mapping <i>vlan-list</i> add-outer <i>outer-vlan-list</i>	Configure the VLAN mapping relationship of port flexible Q-in-Q <i>vlan-list</i> inner: layer VLAN ID from client network <i>outer-vlan-list</i> : added outer layer VLAN ID
4	exit	Return to global configuration mode

5	exit	Return to privileged EXEC mode
6	show vlan mapping	Show all the VLAN mapping configuration
7	show interface port [<i>port-list</i>] switchport	Show port VLAN attribute configuration

Use **no switchport vlan mapping** {all | vlan-list} to delete the VLAN mapping relationship of port Q-in-Q.

△ Notice:

- To ISCOM2924GF/2926, 768 VLAN mapping can be configured at the most.
- The VLAN mapping relationship of flexible Q-in-Q function configure by this command takes effect only on TUNNEL port, that is, only when the interface mode is TUNNEL, can flexible Q-in-Q function takes effect. The port enters command configured outer layer VLAN in the way of UGTAG, if VLAN do not exist, it will be created automatically. When deleting one Q-in-Q VLAN mapping relationship, if other mapping do not user this outer layer VLAN, delete the port from outer layer VLAN.

2.4.3 Monitoring and maintenance

Command	Command parameter instruction
show vlan mapping	Show all the VLAN mapping configuration
show interface port [<i>port-list</i>] switchport	Show port VLAN attribute configuration

2.4.4 Typical configuration example

The topology structure is shown below:

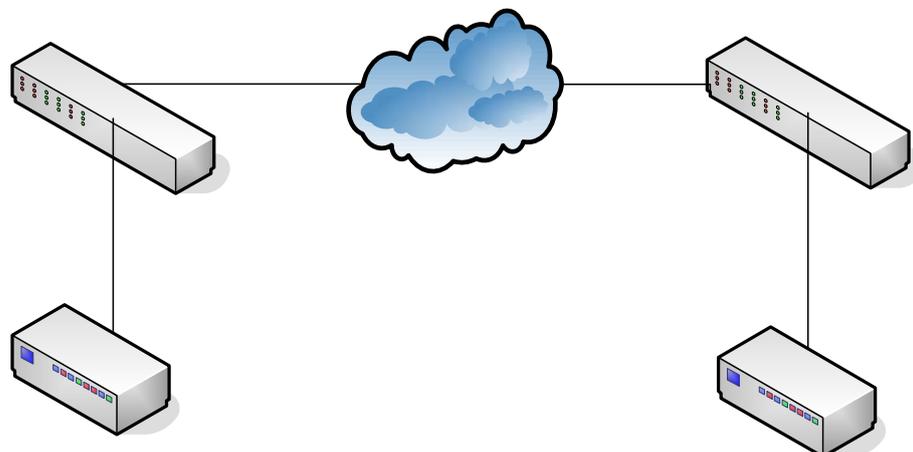


Fig 4 topology structure

As is shown in figure 4, SwitchA and SwitchB are operator access switches, they belong to VLAN 100 and VLAN 200 of the operator’s network respectively. User1 and User2 are user access equipments, SwitchA user P5 port to connect to MAN (metro area network), P1 connect to User1, SwtichB connect to MAN using P5, P1 connect to User2. MAN TPID is 0x8600. User1 belongs VLAN10, User2 belong to VLAN20, configure SwitchA and SwitchB to relalize flexible Q-in-Q function.

SwitchA configure is shown below:

```

Raisecom#config
Raisecom(config)#mls double-tagging tpid 8600
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode dot1q-tunnel
Raisecom(config-port)#switchport vlan mapping 10 add-outer 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 5
Raisecom(config-port)# switchport mode trunk double-tagging
Raisecom(config-port)#exit
Raisecom(config)#exit

```

```

Raisecom#show vlan mapping

```

Port	Inner VLAN	Outer VLAN	Hardware
1	10	100	Yes

```

Raisecom#show interface port 1 switchport

```

```

Port 1:
Administrative Mode: dot1q-tunnel
Operational Mode: dot1q-tunnel
Access Mode VLAN: 4
Tunnel Mode VLAN: 4
Administrative Tunnel Mode OUTER VLANs of vlan mapping: 100
Operational Tunnel Mode OUTER VLANs of vlan mapping: 100
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: n/a
Administrative Hybrid Allowed VLANs: 1-4094
Operational Hybrid Allowed VLANs: n/a
Administrative Hybrid Untagged VLANs: 1

```

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom# show interface port 5 switchport

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,3-6,100

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

SwitichB configuration is shown below:

Raisecom#config

Raisecom(config)#mls double-tagging tpid 8600

Raisecom(config)#interface port 1

Raisecom(config-port)#switchport mode dot1q-tunnel

Raisecom(config-port)#switchport vlan mapping 20 add-outer 200

Raisecom(config-port)#exit

Raisecom(config)#interface port 5

Raisecom(config-port)# switchport mode trunk double-tagging

Raisecom(config-port)#exit

Raisecom(config)#exit

Raisecom#show vlan mapping

Port	Inner VLAN	Outer VLAN	Hardware
1	20	200	Yes

Raisecom#show interface port 1 switchport

Port 1:

Administrative Mode: dot1q-tunnel

Operational Mode: dot1q-tunnel

Access Mode VLAN: 4

Tunnel Mode VLAN: 4

Administrative Tunnel Mode OUTER VLANs of vlan mapping: 200

Operational Tunnel Mode OUTER VLANs of vlan mapping: 200

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: n/a

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Raisecom# show interface port 5 switchport

Port 5:

Administrative Mode: trunk double-tagging

Operational Mode: trunk double-tagging

Access Mode VLAN: 1(default)

Tunnel Mode VLAN: 1(default)

Administrative Tunnel Mode OUTER VLANs of vlan mapping: n/a

Operational Tunnel Mode OUTER VLANs of vlan mapping: n/a

Administrative Trunk Allowed VLANs: 1-4094

Operational Trunk Allowed VLANs: 1,3-6,200

Administrative Hybrid Allowed VLANs: 1-4094

Operational Hybrid Allowed VLANs: n/a

Administrative Hybrid Untagged VLANs: 1

Operational Hybrid Untagged VLANs: n/a

Native Mode VLAN: 1(default)

VLAN Ingress Filtering: Enabled

switchport forwarding allowed portlist: n/a

Chapter 3 VLAN Function Configuration

3.1 Configure VLAN

3.1.2 Switching mode introduction

Switching mode can be sorted to 3 types:

- **transparent** :transparent mode
- **vlan**: VLAN transmission mode
- **double-tagged-vlan**: Q-in-Q VLAN mode

In transparent mode, stable VLAN and port VLAN configuration do not take effect actually. When the system transforms from transparent mode to VLAN transmission mode, stable VLAN and port VLAN configuration can actually take effect.

In VLAN transmission mode, stable VLAN and port VLAN configuration take effect directly. \

3.1.2 Default VLAN configuration

Function	Default value
Create VLAN	Default VLAN
Configure switching mode	Transparent mode
Configure the filtration mode of physical port ingress data packet	No ingress be abandoned.
Configure the data packets that are allowed to be received by physical port	All the data packets are allowed to be received
Configure the handling mode of physical port ingress data packet	No modification to outgress data packet

3.1.3 Configure switching mode

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	switch-mode { transparent dot1q-vlan double-tagged-vlan}	Configure switching mode transparent : transparent mode vlan : VLAN transmission mode double-tagged-vlan : Q-in-Q VLAN

2. Delete VLAN

When user needs to delete a VLAN, follow the steps below:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	no vlan {all <2-4094>}	Delete VLAN <2-4094> VLAN ID; All: all the stable VLAN except default VLAN (VLAN ID is 1)
3	exit	Return to global configuration mode
4	show vlan	Show VLAN configuration

3.1.5 Enable/disable VLAN filtration

The steps to configure the physical port ingress data packet filtration mode are as follows:

Step	Command	Command parameter instruction
1	config	Enter global configuration mode
2	interface {client <i>clientid</i> line <i>lineid</i> }	Enter corresponding physical port configuration mode
3	vlan ingress-filtering {unknown-vlan not-member}	Configure the filtration mode of physical port ingress data packet
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface {client <i>client-list</i> line <i>line-list</i> } switchport	Show VLAN configuration

Use **no vlan ingress-filtering** to restore ingress data packet filtration mode to default value, that is, no ingress packet will be dropped.

3.1.6 Configure VLAN accept-frame tagging type

The steps to configure VLAN accept-frame tagging type are as follows:

Step	Command	Command parameter instruction
1	config	Enter global configuration mode
2	interface {client <i>clientid</i> line <i>lineid</i> }	Enter corresponding physical port configuration mode

3	vlan accept-frame {tag untag}	Configure physical port accepted data packet Tag: accept only the data packets with TAG Untag: accept only the data packet without TAG
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface {client <i>client-list</i> line <i>line-list</i> } switchport	Show VLAN configuration

Use **no vlan accept-frame** to restore VLAN accept-frame tagging type to default value, that is, all the data packets are allowed to receive.

3.1.7 Configure outgress mode

The steps to configure the processing mode of physical port outgress data packet are as follows:

Step	Command	Command parameter instruction
1	config	Enter global configuration mode
2	interface {client <i>clientid</i> line <i>lineid</i> }	Enter corresponding physical interface configuration mode
3	vlan egress default {tag untag unmodify }	Configure the processing mode to physical port outgress data packets Tag outgress data packet adding TAG Untag outgress data packet without TAG Unmodify do not modify outgress data packet
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface {client <i>client-list</i> line <i>line-list</i> }	Show VLAN configuration

switchport

△ Notice:

- If double TAG function is enabled on physical port, the processing mode to physical port outgress data packet will not take effect.

3.1.8 Configure PVID

The steps to create and delete port VLAN ID are shown below:

Step	Command	Command parameter introduction
1	config	Enter global configuration
2	interface {client <i>clientid</i> line <i>lineid</i>}	Enter corresponding physical configuration mode
3	[no] pvid <1-4094> [override]	Create and delete port VLAN ID <1-4094> --- port VLAN ID number Override --- use PVID value to recover the VLAN ID in the message
4	exit	Return to global configuration mode
5	exit	Return to privileged EXEC mode
6	show interface {client <i>client-list</i> line <i>line-list</i>} switchport	Show VLAN configuration

Use **no pvid** to delete PVID.

3.1.9 Monitoring and maintenance

Command	Command parameter introduction
show vlan [<i>{1-4094}</i>]	Show stable VLAN configuration
show interface client [<i>client-list</i>] switchport	Show user port VLAN configuration
show interface line [<i>line-list</i>]	Show line port VLAN

3.1.10 Typical configuration example

Topology structure is shown as figure 5:

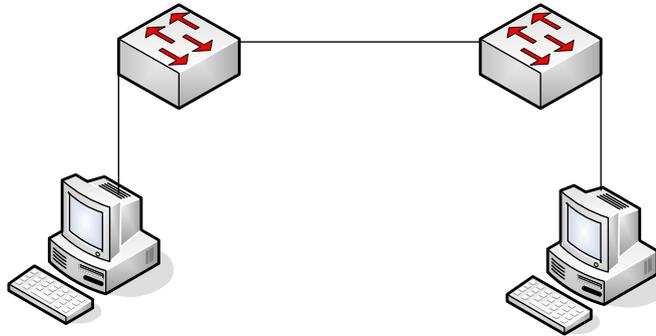


Fig 5 topology structure

Switch A

As is shown in figure 5, Line1 of SwtichB connects with Line1 of SwtichA, configure SwitchA switching mode to vlan transmission mode, and configure Client1 outgress data packet filtration and VLAN accept-frame tagging type.

Client 1

SwitchA configuration is shown below:

```

Raisecom#config
Raisecom(config)#vlan 3 line 1 client 1
Raisecom(config)#switch-mode dot1q-vlan
Raisecom(config)#interface client 1
Raisecom(config-port)#vlan accept-frame untag
Raisecom(config-port)#vlan egress default untag
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show vlan

```

PC1

Switch mode: dot1q-vlan

Core tag type: 0x9100

VLAN	Ports	Untag Ports	Priority
1	L:1;C:1	L:1;C:1	--
3	L:1;C:1	n/a	--

```

Raisecom#show interface client 1 switchport

```

Port client1:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: Untagged

Vlan ingress filtering: None

Egress default : Untagged

SwitchB configuration is shown below:

Raisecom#config

Raisecom(config)#**vlan 3-5 line 1 client 1**

Raisecom(config)#**switch-mode dot1q-vlan**

Raisecom(config)#**interface client 1**

Raisecom(config-port)#**vlan accept-frame untag**

Raisecom(config-port)#**vlan egress default untag**

Raisecom(config-port)#**exit**

Raisecom(config)#**exit**

Raisecom#show vlan

Switch mode: dot1q-vlan

Core tag type: 0x9100

VLAN	Ports	Untag Ports	Priority
1	L:1;C:1	L:1;C:1	--
3	L:1;C:1	n/a	--
4	L:1;C:1	n/a	--
5	L:1;C:1	n/a	--

Raisecom#show interface client 1 switchport

Port client1:

PVID: 1

PVID override: Disabled

Double tag: Disabled

Vlan accept-frame: Untagged

Vlan ingress filtering: None

Egress default : Untagged

3.2 Basic Q-in-Q function

3.2.1 Basic Q-in-Q default configuration

Function	Default value
Configure outer layer Tag TPID value	The default TPID value of outer layer Tag is 0x9100
Enable/disable physical port double TAG function	Double TAG function is disabled

3.2.2 Configure basic Q-in-Q

Q-in-Q configuration includes: switching mode, Tpid, PVID and double tagging configuration, the configuration steps are as follows:

Step	Command	Command parameter introduction
1	config	Enter global configuration mode
2	switch-mode { transparent dot1q-vlan double-tagged-vlan}	Configure switching mode to double-tagged-vlan mode Transparent: transparent mode Vlan: VLAN Transmission mode double-tagged-vlan: Q-in-Q VLAN mode
3	mls double-tagging tpid HHHH	Configure outer layer Tag TPID value to HHHH HHHH: hex outer layer Tag TPID value, which is 1~4 figures hex number, range is 0x0-0xFFFF
4	interface {client <i>clientid</i> line <i>lineid</i>}	Enter corresponding physical interface configuration mode
5	pvid <1-4094> [override]	Create port VLAN ID <1-4094>——port VLAN id Override——use PVID value to recover message VLAN ID
6	vlan double-tag	Enable physical port double TAG function

7	exit	Return to global configuration mode
8	exit	Return to privileged EXEC mode
9	show vlan	Show stable VLAN configuration
10	show interface {client client-list line line-list} switchport	Show VLAN configuration

Use **no mls double-tagging tpid HHHH** to restore outer layer Tag TPID to default value, 0x9100.

Use **no vlan double-tag** to stop physical port double TAG function.

3.2.3 Monitoring and maintenance

Command	Command parameter introduction
show vlan [{1-4094}]	Show stable VLAN configuration
show interface client [client-list] switchport	Show user port VLAN configuration
show interface line [line-list] switchport	Show line port VLAN configuration

3.2.4 Typical configuration example

Topology structure:

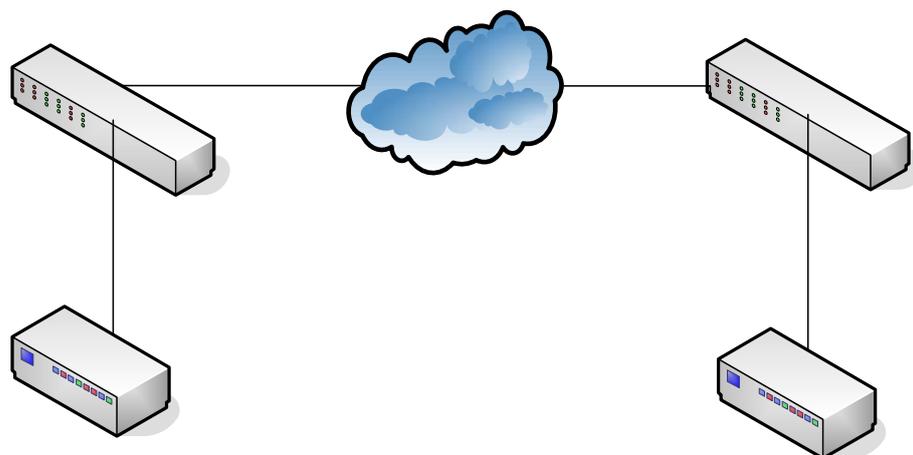


Fig 6 topology structure

As is shown in the topology structure, SwitchA and SwitchB are operator access switches, which belongs to VLAN100 and VLAN200 of the operator network. User1 and User2 are user access equipments, SwitchA use P5 to connect to MAN (metro area network), P1 connect to User1,

SwitchB use P5 to connect to MAN, P1 connect to User2. Among them, MAN TPID is 0x9600. Configure SwtichA and SwtichB to realize basic Q-in-Q function.

SwitchA configuration is as follows:

```

Raisecom#config
Raisecom(config)#switch-mode double-tagged-vlan
Raisecom(config)#mls double-tagging tpid 9600
Raisecom(config)#interface client 3
Raisecom(config-port)#pvid 100
Raisecom(config-port)#vlan double-tag
Raisecom(config-port)#exit
Raisecom(config)#exit
Raisecom#show vlan

```

Switch mode: double-tagged-vlan

Core tag type: 0x9600

VLAN	Ports	Untag Ports	Priority
1	L:1;C:1-4	L:1;C:1-4	--
3	C:3	n/a	--
5	L:1	n/a	--

```

Raisecom#show interface client 3 switchport

```

```

Port client3:
PVID: 100
PVID override: Disabled
Double tag: Enabled
Vlan accept-frame: All
Vlan ingress filtering: None
Egress default : Unmodify

```

SwitchB 配置如下:

```

Raisecom#config
Raisecom(config)#switch-mode double-tagged-vlan
Raisecom(config)#mls double-tagging tpid 9600
Raisecom(config)#interface client 3
Raisecom(config-port)#pvid 200

```

```
Raisecom(config-port)#vlan double-tag
```

```
Raisecom(config-port)#exit
```

```
Raisecom(config)#exit
```

```
Raisecom#show vlan
```

```
Switch mode: double-tagged-vlan
```

```
Core tag type: 0x9600
```

```
VLAN   Ports           Untag Ports  Priority
```

```
-----
```

VLAN	Ports	Untag Ports	Priority
1	L:1;C:1-4	L:1;C:1-4	--
5	L:1	n/a	--
6	C:2	n/a	--

```
Raisecom#show interface client 3 switchport
```

```
Port client3:
```

```
PVID: 200
```

```
PVID override: Disabled
```

```
Double tag: Enabled
```

```
Vlan accept-frame: All
```

```
Vlan ingress filtering: None
```

```
Egress default : Unmodify
```



北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056
Email: export@raisecom.com <http://www.raisecom.com>